Raytheon

October 2002

Dr. Dan Surber
Principal Systems Engineer
Ms. Mary Randall
Senior Systems Engineer
Raytheon Technical Services Company

Certification of Legacy Military A/C Software

Raytheon

Overview

- **DOD-STD-2167A vs DO-178**
- **Options for Legacy Software**
- **Obtaining Cert Authority Concurrence**
- **Other Issues**
- **Q&A**

Raytheon

Software Standards

- **Current commercial standard is RTCA DO-178B**
- **Some Legacy commercial systems developed to DO-178A**
- **Many legacy military systems developed to DOD-STD-2167A (or 1679)**

Raytheon

Legacy vs DO-178B

FAA Notice N8110.89

- **Provides guidelines for approval of software changes in legacy software using DO-178B**
- **Specifically addresses software developed to earlier versions of DO-178**
- **Does not mention DOD-STD-2167**
- **Electronic Systems Command was interested in mapping 2167 to 178 (not funded)**

Raytheon

Possible Approaches

OPTION 1

- **Map DOD-2167A to DO-178A**
- **Assess legacy system to DO-178A criteria**
  - **Establish equivalency defined to DO-178A software level**
- **Use FAA guidance for DO-178A vs DO-178B mapping and analysis**
- **Evaluate “gaps” to 178B**
- **Plan actions & execute plan**
- **Close “gaps” and document method & results**

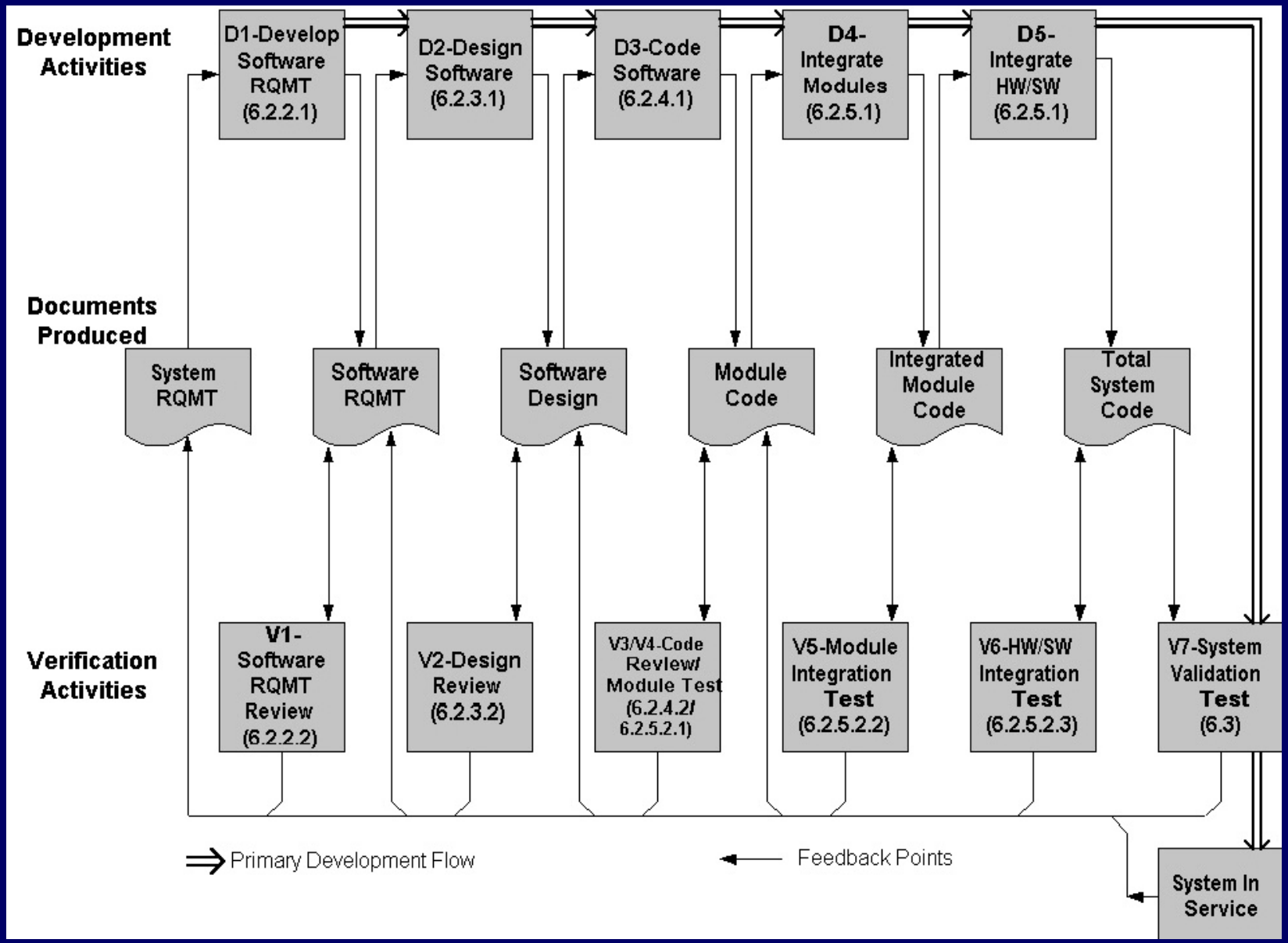
OPTION 2

- **Determine level of design assurance needed under 178B for legacy software**
- **Use DO-178B and legacy software documentation to do a “Gap Analysis”**
- **Determine actions to close “gaps” based upon level of design assurance needed**
- **Close “gaps” and document method & results**

ESC & Boeing using Opt.2

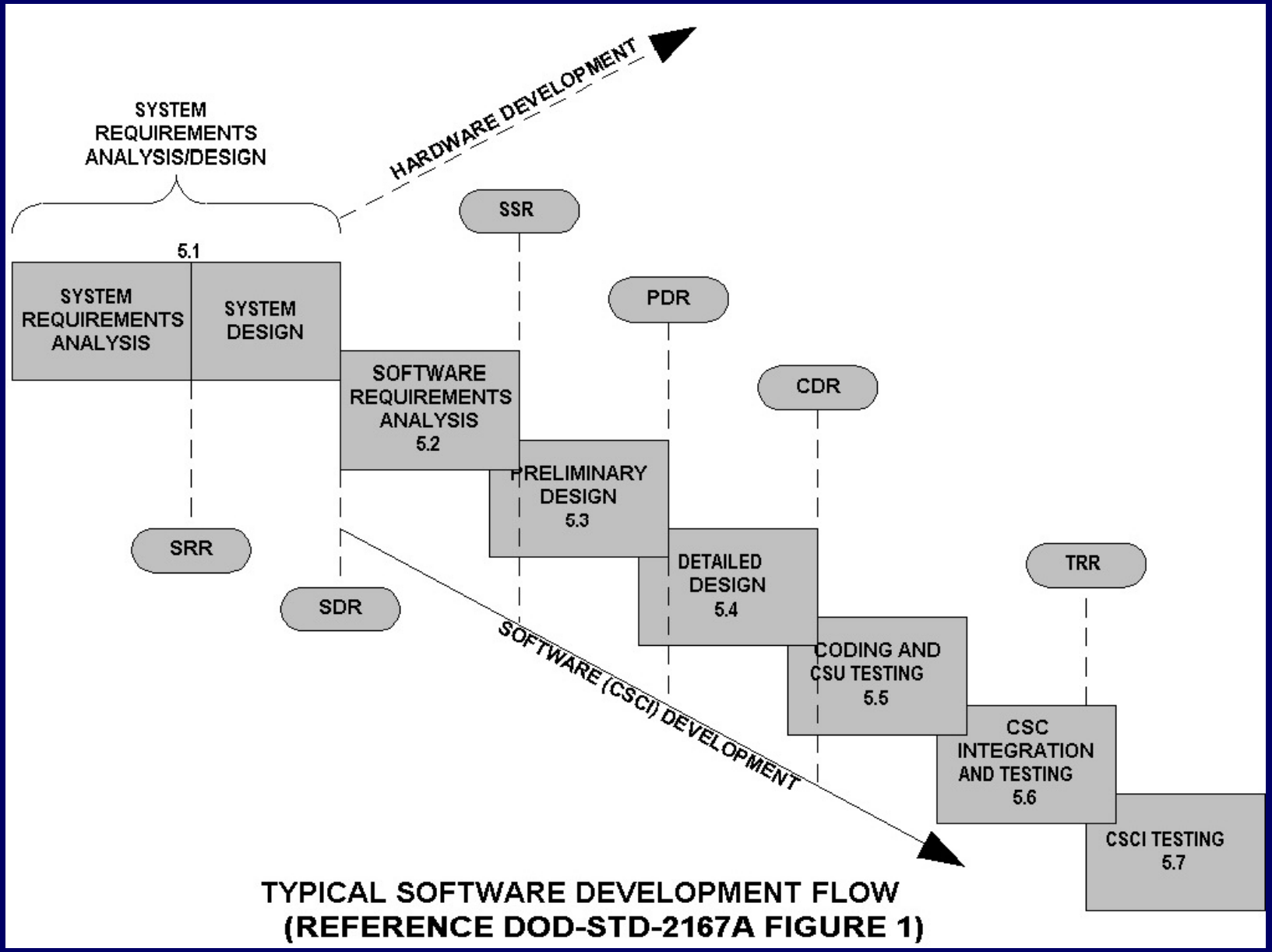
DO-178A Defined Software Development & Verification Activities

Raytheon



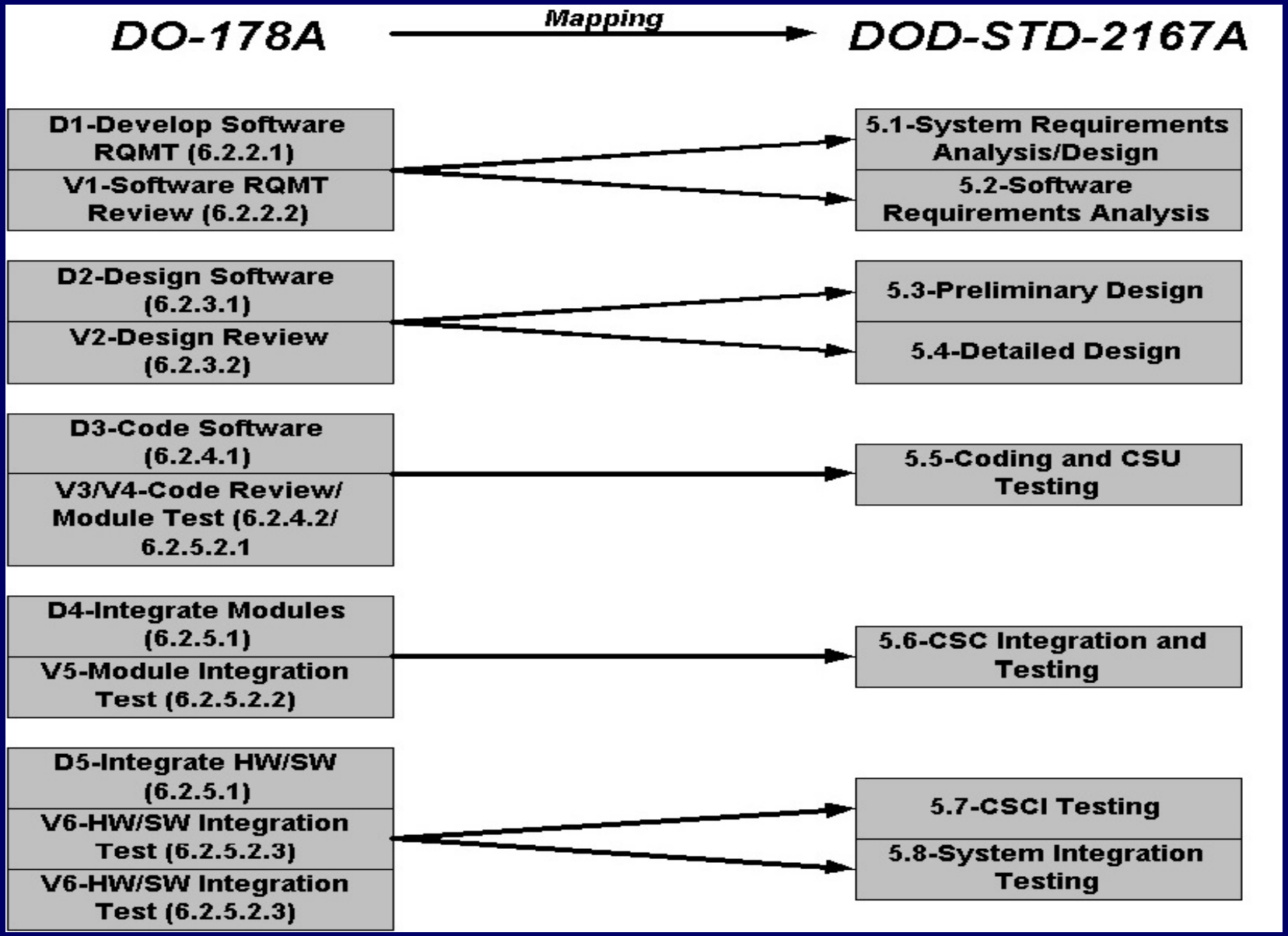
Raytheon

Typical Software Development Flow



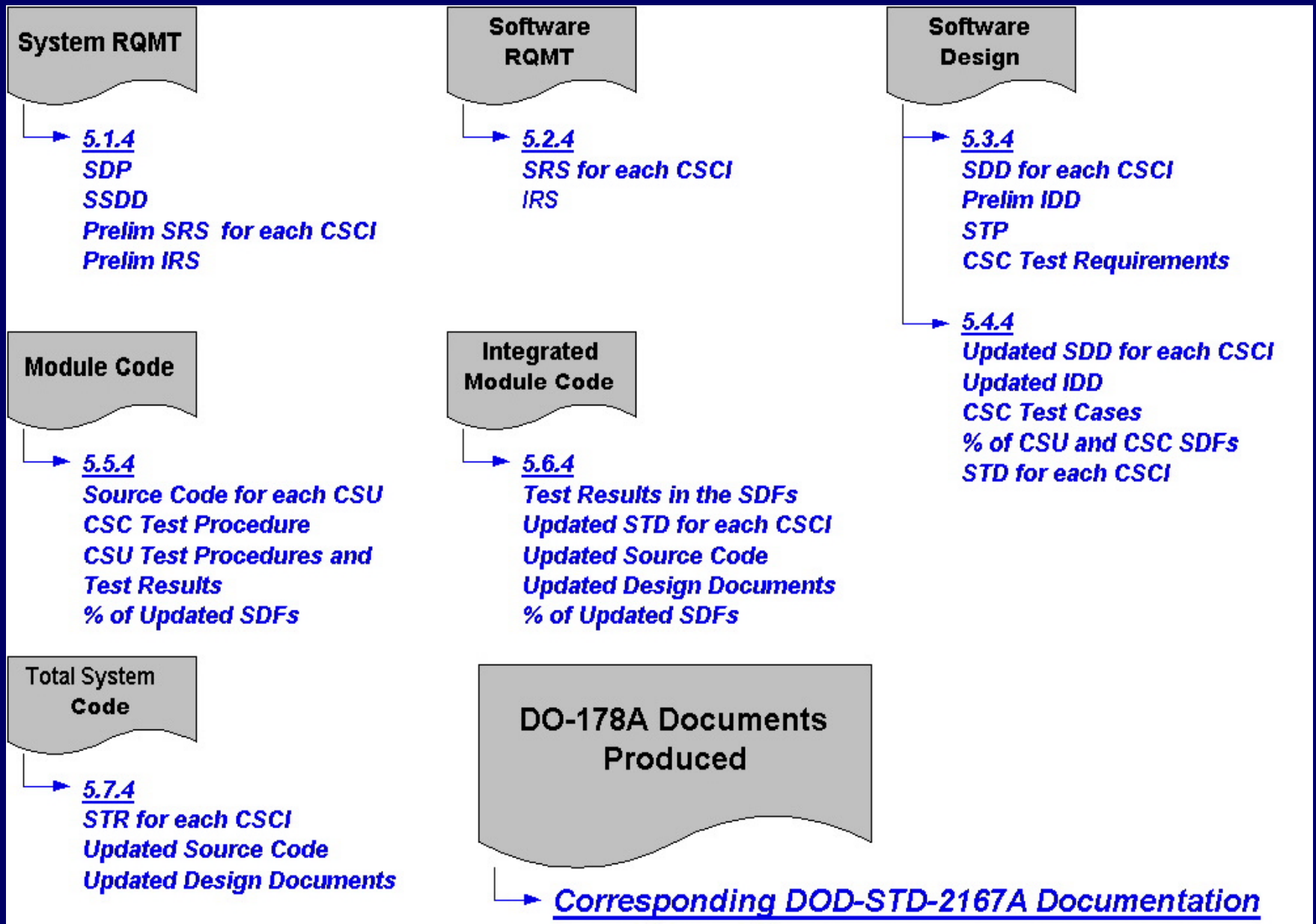
TYPICAL SOFTWARE DEVELOPMENT FLOW
(REFERENCE DOD-STD-2167A FIGURE 1)

Mapping


DO-178A
Mapping
DOD-STD-2167A
D1-Develop Software RQMT (6.2.2.1)
V1-Software RQMT Review (6.2.2.2)
5.1-System Requirements Analysis/Design
5.2-Software Requirements Analysis
D2-Design Software (6.2.3.1)
V2-Design Review (6.2.3.2)
5.3-Preliminary Design
5.4-Detailed Design
D3-Code Software (6.2.4.1)
V3/V4-Code Review/ Module Test (6.2.4.2/ 6.2.5.2.1
5.5-Coding and CSU Testing
D4-Integrate Modules (6.2.5.1)
V5-Module Integration Test (6.2.5.2.2)
5.6-CSC Integration and Testing
D5-Integrate HW/SW (6.2.5.1)
V6-HW/SW Integration Test (6.2.5.2.3)
V6-HW/SW Integration Test (6.2.5.2.3)
5.7-CSCI Testing
5.8-System Integration Testing

Raytheon

Process



Raytheon

Cert Authority Concurrence

- **Identify Cert Authority**
- **Present a plan based on Options 1 or 2**
- **Be clear on tailoring done for 2167**
- **Have traceability of requirements thru design & testing documents**
- **Be clear about “gaps” in meeting level of design assurance “targeted” in 178B & planned closure**
- **Follow through with the plan**
- **Document results**

Raytheon

Other issues

- **Certification only covers the software**
- **Safety considerations in system architecture**
- **Design assurance for hardware and total system is more than meeting 178B**
- **Recommend same approach noted in Options 1 or 2**
- **Legacy systems will continue to change, how will future changes be accounted for in “gap” analysis, closure and design assurance after initial effort?**
- **Who does any software/system safety analysis and impact assessment for these changes?**

Raytheon

Sources Used

- RTCA/DO-178B/ED-12B: “Software Considerations in Airborne Systems and Equipment Certification,” Dec 1992.
- FAA Position Paper, CAST-9: “Considerations for Evaluating Safety Engineering Approaches to S/W Assurance,” Jan 2002.
- Leslie A. Johnson (Boeing): “DO-178B Software Considerations in Airborne Systems and Equipment Certification”, Feb 2002.
- Leanna K. Rierson (FAA): “Using the Software Capability Maturity Model for Certification Projects,” date unknown.
- RTCA/DO-178A: “Software Considerations in Airborne Systems and Equipment Certification”, March 22, 1995
- FAA Notice N8110.89: “Guidelines For the Approval of Software Changes in Legacy Systems Using RTCA DO-178B”, Jan 16, 2001
- DOD-STD-2167A: “Defense System Software Development”, Feb 29, 1988

Questions?